

Application No.: 09/940,706
Filing Date: 08/28/2001

RECEIVED
CENTRAL FAX CENTER

MAY 07 2007

Docket No.: JP920010196US1

REMARKS

Please enter the amendments set out herein above to delete the word "improved" in claims 2, 4, and 5. The amendment is in compliance with Examiner's objection.

General remarks

The present application describes issues arising from the increasing number of credentials that are required for conducting business on-line as e-business evolves and progresses. In the "Background of the invention," the application explains on pages 1 and 2 that a certificate for each credential may be obtained from a certification authority, and that while this permits less exposure of a given credential to applications having no relation to that credential, this arrangement with multiple certificates presents maintenance issues. The present application goes on to explain on pages 2 and 3 that one alternative is to include numerous credentials in a single certificate from a certification authority, but that this also causes problems. For example, this increases certificate size, causing delays in handshakes.

The present application goes on to describe a solution that brings more flexibility to handshakes. According to an aspect of the teachings in the present application, one certificate with a set of credentials is issued by an authority, and then other, self-certified credentials required during transactions are generated and signed by the participant itself. See, for example, present application page 3 (referring to a certificate with validity status dates and a set of credentials as "basic authentication data" and to a self-certified certificate with validity status dates and a credential as "additional individual authentication data units"). See also, page 6 (certificate with validity status dates and a set of numerous credentials, i.e., SSL server, email signer, email recipient and status responder); page 8 (self generated certificate with validity status dates and a credential for email); and page 7, first paragraph ("Client applications . . . can also generate these certificates on the fly in case the CA signature is not required.").

Datar also concerns certificates. However, Datar concerns ways to determine a certificate's "revocation status," which Datar also refers to as "validity." See, e.g., Datar, col. 1, lines 41-56. Datar explains that certificate validation has conventionally been done, in one alternative, by searching through certificate revocation lists ("CRL's"). See, e.g., Datar, col. 1, line 57 - col. 2, line 9 (describing an associated set of drawbacks). Datar explains that another alternative has conventionally been a "real-time" inquiry. See, e.g., Datar, col. 2, lines 10-54

Application No.: 09/940,706
Filing Date: 08/28/2001

Docket No.: JP920010196US1

(describing this validation approach and another set of drawbacks). A third conventional alternative disclosed by Datar concerns short-lived certificates. See, e.g., Datar, col. 2, line 55 - col. 3, line 2. (describing this validation approach and another set of drawbacks).

Datar describes several alternatives in addition to the conventional ones. See, e.g., Datar, col. 3, line 52 - col. 4, line 22 (describing three alternative embodiments). Datar makes the point that all three embodiments are advantageous because they involve a user *caching* its own certificate status information and because they involve "application-appropriate" policies regarding revocation "freshness," i.e., policies that may vary according to the context of different software applications. Datar, col. 4, lines 36-51.

Notice, however, although Datar teaches that the user *caches* its own certificate status information, the certificate status information is *generated by and obtained from the certificate authority in every case*. See, Datar, col. 3, line 64 (first embodiment); col. 4, lines 7-8 (second embodiment); and col. 4, lines 19-20 (third embodiment). See also, Datar, col. 6, lines 37-59 (user gets certificate status cookie 28 from certificate status authority 26); col. 8, lines 8-30 (user gets associate status cookie 36 from associate status authority 32).

Claims 1-15 stand rejected under 35 USC 102(e) as being anticipated by Datar (US Patent 6,351,812). Claims are amended herein to overcome the rejection by more clearly pointing out novel and nonobvious distinctions of the present invention. No new matter is added, since the original application provides support for the amendments, as described herein below. The amendments herein also change the claims to set out elements, steps and limitations from the point of view of the first computer, i.e., a computer that accesses applications on or from a second computer.

Claims 1, 6 and 11

Like Datar, the present application teaches that basic authentication data for a first computer is certified by an accepted certifying authority and is sent from the first computer to a second computer for permitting a first type of secure transaction access by the first computer to an application provided by the second computer. However, unlike Datar, and as explained above, an additional individual authentication data unit is *generated by the first computer*, according to the present application. Present application, page 7, first paragraph. The first computer signs the individual authentication data unit using a key associated with its public key

Application No.: 09/940,706
Filing Date: 08/28/2001

Docket No.: JP920010196US1

and sends the additional individual authentication data to the second computer. Present application, page 8, last paragraph ("signature on the USC . . . is of the client"). Thus, the second computer can verify authenticity of the additional individual authentication data unit using the first computer's public key that was received from the first computer by the second computer with the basic authentication data. Present application, page 8, last paragraph ("signature on the USC . . . can be verified by the server"). In order to make this distinction all the more clear in the claims of the present application, claims 1, 6 and 11 are herein amended to more particularly point out the above described features. For example, claim 1, as amended herein states that the additional individual authentication data unit is generated and signed by the first computer, so that the second computer can verify authenticity of the additional individual authentication data unit using the first computer's public key that was received from the first computer by the second computer with the basic authentication data. Claims 6 and 11 are similarly amended, each according to the forms of the invention they claim. The cited art does not teach or suggest this.

Further, the "basic authentication data" provides a credential and *not merely a validation status* for permitting a first type of secure transaction access by the first computer to an application provided by the second computer. See, e.g., "current certificate" on page 6 of the present application, which includes a validation date. Likewise, the "additional individual authentication data unit" provides a credential and not merely a validation status for permitting a second type of access by the first computer to an application provided by the second computer. See, e.g., present application, pages 7 and 8, "e-mail unit self certificate" and paragraph following. Moreover this can be done during the same certain communication session. See, e.g., present application, page 3, last paragraph.

Datar col. 7, lines 32-64, is cited regarding an additional individual authentication data unit for permitting a second type of access by the first computer to an application provided by the second computer during the same certain communication session. However, what Datar teaches in this passage concerns merely "refreshing" a validation cookie, not presenting an additional credential to an application server for permitting a second type of access by the first computer to an application provided by the second computer during the same certain communication session. The present application gives an example on page 1 regarding SSL communication in which changing *credentials* in the conventional manner, i.e., a manner in which a certifying authority

Application No.: 09/940,706
Filing Date: 08/28/2001

Docket No.: JP920010196US1

must be involved, requires initiating a new session. See, e.g., present application, page 1, lines 19-26 (discussing breaking a session, such as by closing a browser, in order to get a server to accept another certificate).

In order to make the above distinctions all the more clear in the claims of the present application, claim 1 is herein amended to more particularly point out that "the basic authentication data provides a certificate including a validity status date and a credential, the credential being for permitting a first type of transaction access by the first computer to an application provided by the second computer" and "the additional individual authentication data unit provides a self certificate including a validity status date and a credential, the self certificate credential being for permitting a second type of access by the first computer to an application provided by the second computer." Claims 6 and 11 are similarly amended, each according to the forms of the invention they claim. The cited art does not teach or suggest this.

Claims 2, 4, 7, 9, 12 and 14

Claims 2, 4, 7, 9, 12 and 14 were previously amended to state specific *types* of access permitted responsive to additional individual authentication data units and pointed out that the cited art does not teach or suggest these types of access are permitted responsive to additional authentication data units received individually, i.e., separately from basic authentication data received for a first type of access during the same session. In reply the present Office action presents arguments regarding elements, steps or limitations of claims 1, 6 and 11, but does not address the particular types of access set out in claims 2, 4, 7, 9, 12 and 14. Applicant submits that claims 2, 4, 7, 9, 12 and 14 are patentably distinct because the cited art does not teach or suggest these types of access are permitted responsive to additional authentication data units received individually, i.e., separately from basic authentication data received for a first type of access during the same session, as claimed.

Further, Applicant submits that claims 2, 4, 7, 9, 12 and 14 are patentably distinct because they respectively depend upon allowable claims. MPEP 2143.03 ("If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious," citing *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)).

Application No.: 09/940,706
Filing Date: 08/28/2001

RECEIVED
CENTRAL FAX CENTER
Docket No.: JP920010196US1

MAY 07 2007

Claims 3, 5, 8, 10, 13 and 15

Datar col. 7, lines 32-64 is cited regarding "receiving . . . a command . . . for the second computer to invalidate a previously presented identity certificate; and receiving . . . a new identity certificate from the first computer to replace the invalidated identity certificate, wherein the command to invalidate and the new identity certificate are both received by the second computer during the certain communication session." Applicant submits that the cited teaching does not teach or suggest this for reasons set out above in the discussion of this passage of Datar. In addition, claims 5, 10 and 15 are herein amended to emphasize and more particularly point out the novel and nonobvious distinction that "the previously presented identity certificate includes a validity status date and an identity credential" and that a new identity certificate is *generated* and sent by the first computer and has "a validity status date and an identity credential . . . to replace the invalidated identity certificate, wherein the command to invalidate and the new identity certificate are both received by the second computer during the certain communication session."

Further, Applicant submits that claims 3, 5, 8, 10, 13 and 15 are patentably distinct because they respectively depend upon allowable claims. MPEP 2143.03 ("If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious," citing *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)).

REQUESTED ACTION

Applicant contends that the invention as claimed in accordance with amendments submitted herein is patentably distinct, and hereby requests that Examiner grant allowance and prompt passage of the application to issuance.

Respectfully submitted,



Anthony V. S. England
Attorney for Applicants
Registration No. 35,129
512-477-7165
a@aengland.com